

2. Простым языком об HTTP [Электронный ресурс] // Хабрахабр. Режим доступа: <https://habrahabr.ru/post/215117/> (дата обращения: 08.11.2017).
3. Cookies [Электронный ресурс] // Cyberguru. Режим доступа: <http://www.cyberguru.ru/dotnet/asp-net/cookies-beginners.html> (дата обращения: 08.11.2017).
4. Cookie: что нужно знать? [Электронный ресурс] // Kaspersky lab Daily. Режим доступа: <https://www.kaspersky.ru/blog/cookie-cto-nuzhno-znat/979/> (дата обращения: 08.11.2017).
5. Уязвимости веб-приложений: пора анализировать исходный код [Электронный ресурс] // Positive Research. Режим доступа: <http://blog.ptsecurity.ru/2017/08/web-attacks.html> (дата обращения: 08.11.2017).
6. Хмельникова О. А., Чудинова Е. В. Обеспечение безопасности онлайн-покупок // Сб. тезисов докладов науч.-практ. конф. студентов Курган. гос. ун-та. Курган : Изд-во Курганского гос. ун-та, 2016. Вып. 17. С. 50.
7. Скоробогатов Д. А., Москвин В. В. Безопасность электронных платежных систем на примере PayPal // Сб. материалов XV Всерос. науч.-практ. конф. студентов, аспирантов и молодых ученых «Безопасность информационного пространства». Курган, Курганский государственный университет, 2016. С. 202–205.
8. Не все cookie одинаково полезны [Электронный ресурс] // Хабрахабр. Режим доступа: <https://habrahabr.ru/post/272187/> (дата обращения: 08.11.2017).

УДК 004.056.5

**Е. Ю. Мищенко**

Научный руководитель: канд. тех. наук, доц. А. Н. Соколов  
Южно-Уральский государственный университет, Челябинск

## **ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ КАК СПОСОБ СНИЖЕНИЯ ЗАТРАТ НА СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ**

*Аннотация.* Обезличивание персональных данных как метод их защиты требует методологического обеспечения не только в плане подхода к реализации, но также в части обоснования эффективности как функциональной, так и экономической. В данной работе предлагается обоснование эффективности применения метода введения идентификаторов на основе критерия вероятности идентификации и рассматривается подход к реализации данного метода на базе запатентованной полезной модели. В результате внедрения метода в сфере здравоохранения был получен значительный экономический эффект.

*Ключевые слова:* персональные данные; обезличивание; метод идентификаторов.

**Введение.** Защите персональных данных уделяется большое значение во многих странах. Соответствующие нормативные акты уже в конце прошлого века были приняты в США [1] и ЕС [2]. В начале нашего века были разработаны методы защиты персональных данных, в том числе методы обезличивания. В соответствии со стандартами США [3] и Великобритании [4] главной целью обезличивания является обеспечение заданной степени невозможности раскрытия персональных данных (анонимизации), в чем были достигнуты значительные успехи. В то же время вопросу обеспечения их полноценного восстановления не уделялось достаточного внимания. Например, методам анонимизации посвящено 9 из 10 работ по обезличиванию как западных (США, ЕС), так и других (Корея, Индия, Китай) исследователей. Наша страна в этом отношении является исключением, поскольку в законе «О персональных данных» [5] понятие обезличивания определяется как способ обработки, при котором невозможно без дополнительной информации определить принадлежность персональных данных физическому лицу, а все методы обезличивания, определенные в Приказе Роскомнадзора России № 996 [6], предполагают возможность восстановления персональных данных. Похожие работы иностранных исследователей гарантируют полноценную работу с обезличенными данными только при использовании криптографии [7].

Приказ Роскомнадзора России определяет четыре метода обезличивания (введение идентификаторов, изменение состава или семантики, декомпозиция, перемешивание) [6]. С точки зрения результатов обезличивания, метод введения идентификаторов представляется наиболее простым, поскольку в отличие от других методов не требует применения сложного математического аппарата, а требует «простого» разделения базы данных на «идентификаторы» и «прочие данные», которые и являются обезличенными. Видимо, поэтому большинство российских исследователей уделяют внимание «более интересным» с точки зрения разработки методам — изменению состава или семантики (наиболее близкий аналог анонимизации) и перемешиванию (тоже используется в анонимизации, но реже). Например, алгоритмы перемешивания предлагают В. А. Козлов [8] и И. П. Карпова [9], изменения состава или семантики — И. Ю. Кучин [10] и Ю. В. Трифонова [11]. Но самая серьезная проблема в реализации любого метода обезличивания состоит в обеспечении недоступности дополнительной информации (идентификаторов или алгоритмов модификации/перемешивания) в сеансе работы с обезличенными данными. По состоянию на сегодняшний день реализация обезличивания в промышленном масштабе достигнута только с применением метода введения идентификаторов — в сфере образования (Е. С. Волокитина [12] на базе полезной модели) и в сфере здравоохранения (А. А. Кошкарров, А. А. Халафян [13]). Однако упомянутые реализации вынужденно используют либо дополнительное оборудо-

вание, либо средства криптографической защиты, что не позволяет добиться полного экономического эффекта.

В данной работе представлена реализация метода введения идентификаторов в сфере здравоохранения на базе полезной модели, а также метод оценки эффективности обезличивания на основе критерия вероятности идентификации.

**Методы.** Метод введения идентификаторов был реализован на базе полезной модели «Система взаимодействия разделенных баз персональных данных информационной системы» (патент № 103414 от 02.12.2010), отличительной особенностью которой является использование внешнего идентификатора для связи таблицы перекрестных ссылок с обезличенной частью базы. В идеальном варианте это носитель, уже используемый в технологическом процессе. Поскольку методика предполагает хранение таблицы перекрестных ссылок на защищенном сервере при невозможности доступа к ней с удаленных рабочих мест, для внедрения необходимо произвести модернизацию структуры и исполняемых процедур базы данных и, возможно, программного интерфейса, что возможно только в случае доступа к исходным текстам программного обеспечения. Методика оценки эффективности обезличивания представляет собой итерационную процедуру, подробно описанную автором данной работы в [14] и состоящую из этапов:

- 1) выбор группы наиболее чувствительных идентифицирующих атрибутов и перенос их в таблицу перекрестных ссылок;
- 2) определение критерия вероятности идентификации ВИ как максимальной обратной величины результата выполнения запроса по любой группе оставшихся реквизитов в обезличенной базе;
- 3) в неудовлетворительном случае происходит возврат к п. 1.

**Результаты.** Апробация метода проводилась в базе данных льготного лекарственного обеспечения Челябинской области, с центром обработки данных в г. Челябинске и удаленными рабочими местами в более 100 аптечных пунктах в районах и городах области, причем в качестве внешнего идентификатора использовался рецепт на машиночитаемом бумажном носителе. Следовательно, в отличие от решений, предлагаемых в [12] и [13], дополнительных внешних идентификаторов и средств защиты информации на удаленных рабочих местах (значит, и связанных с ними затрат) не потребовалось. При внедрении была произведена модернизация структуры и исполняемых процедур базы данных, а также программного интерфейса оператора, согласно разработанному техническому заданию. Определение критерия вероятности идентификации ВИ производилось для нескольких групп реквизитов из обезличенной базы. Результаты внедрения показали, что при переносе всех чувствительных идентифицирующих атрибутов технологический процесс обработки инфор-

мации не был нарушен, причем вероятность идентификации не превышала обратной величины пациентов с конкретным диагнозом.

**Заключение.** Использование указанных выше методик обезличивания показало их технологическую и функциональную эффективность, а также позволило сэкономить более 1 млн руб. на средствах защиты информации для удаленных рабочих мест, поскольку согласно закону [5] обезличенные данные не попадают под определение персональных данных и не требуют защиты при их обработке.

### Список литературы

1. Privacy Protection Act of 1980 OCT. 13, 1980 [Электронный ресурс]. URL: <https://www.govtrack.us>.
2. Конвенция о защите физических лиц при автоматизированной обработке персональных данных. Страсбург. 28.01.1981. [Электронный ресурс]. URL: <http://www.consultant.ru>.
3. Guide to Protecting the confidentiality of Personally Identifiable Information (PII) SP 800–122, 2010 [Электронный ресурс]. URL: <http://nvlpubs.nist.gov>.
4. Anonymisation: managing data protection risk. Code of practice. Information Commissioner's Office, November 2012 [Электронный ресурс]. URL: <https://ico.org.uk>.
5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [Электронный ресурс]. URL: <http://www.consultant.ru>.
6. Приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» [Электронный ресурс]. URL: <http://www.garant.ru>.
7. Shehu B., Ahmetaj Sh., Aranitasi M., Xhuvani A. Protection of Personal Data in Information Systems // International Journal of Computer Science Issues. 2013. Vol. 10. Is. 4. No 2. P. 78–81.
8. Бондаренко К. О., Козлов В. А. Универсальный быстродействующий алгоритм процедур обезличивания данных // Изв. ЮФУ. Технические науки. 2015. № 11 (172). С. 130–142.
9. Карпова И. П. О реализации метода обезличивания персональных данных // Вестн. компьютерных и информационных технологий. 2013. № 6. С. 56–60.
10. Кучин И. Ю. Обработка баз данных с персонифицированной информацией для задач обезличивания и поиска закономерностей : дис. ... канд. тех. наук. Астрахань, 2012 [Электронный ресурс]. URL: <http://www.dissercat.com>.
11. Трифонова Ю. В. Возможности обезличивания персональных данных в системах, использующих реляционные базы данных // Доклады ТУСУР. 2014. № 2 (32). С. 188–194.

12. Волокитина Е. С. Метод и алгоритмы гарантированного обезличивания и реидентификации субъекта персональных данных в автоматизированных информационных системах : дис. ... канд. тех. наук. Санкт-Петербург, 2013 [Электронный ресурс]. URL: <http://www.dissercat.com>.

13. Халафян А. А., Кошкарлов А. А. Система управления базами данных льготного лекарственного обеспечения в Краснодарском крае с использованием облачных технологий // Политематический сетевой электрон. науч. журнал Кубан. гос. аграр. ун-та, 2015. № 109 (05). С. 451–467.

14. Мищенко Е. Ю., Соколов А. Н. Количественный анализ процедуры обезличивания персональных данных. Метод введения идентификаторов // Вестн. Южно-Урал. гос. ун-та. Серия: Компьютерные технологии, управление, радиоэлектроника. Челябинск : Изд. центр ЮУрГУ, 2015. № 3. С. 18–25.

УДК 004.056

П. О. Садков, С. П. Новокшенова, А. Е. Шлемов, А. А. Пермяков

Научный руководитель: канд. тех. наук, доц. Т. Ю. Зырянова

Уральский государственный университет путей сообщения, Екатеринбург

## ИНТЕРНЕТ-МЕМЫ КАК ОРУЖИЕ ИНФОРМАЦИОННОЙ ВОЙНЫ

*Аннотация.* В статье приведены результаты исследования влияния социальных сетей, в первую очередь интернет-мемов, на современное общество. Рассмотрено понятие интернет-мемов, способы их воздействия на человека. Проведен опрос людей различных возрастов.

*Ключевые слова:* интернет-мем; социальные сети; контент; информационная безопасность.

В современном обществе влияние социальных сетей с каждым годом все увеличивается. Если раньше основным источником информации были книги, телепередачи и газетные издания, которые подвергались цензуре, то так называемые интернет-мемы циркулируют в интернет-среде абсолютно бесконтрольно, что представляет потенциальную угрозу информационной безопасности РФ.

Термин «мем» (от греч. «мимема» — подобие) впервые употребил оксфордский профессор, биолог Ричард Докинз. Он провел аналогию между генами, которые формируют человека как живое существо, и мемами, которые формируют человека как существо социальное [1]. В широком понимании мем — это